

Operating Systems
Professor Ward
Spring 2021

Packet Inspection Assignment

Download and install Wireshark. Run it, select an interface with traffic, and start capturing packets. Do a ping, plus a whois or anything else to generate network traffic. Stop the capture.

1. Show a screenshot of Wireshark at the end.
2. How many packets did it capture? What was the packets-per-second rate?

→ 7766 packets

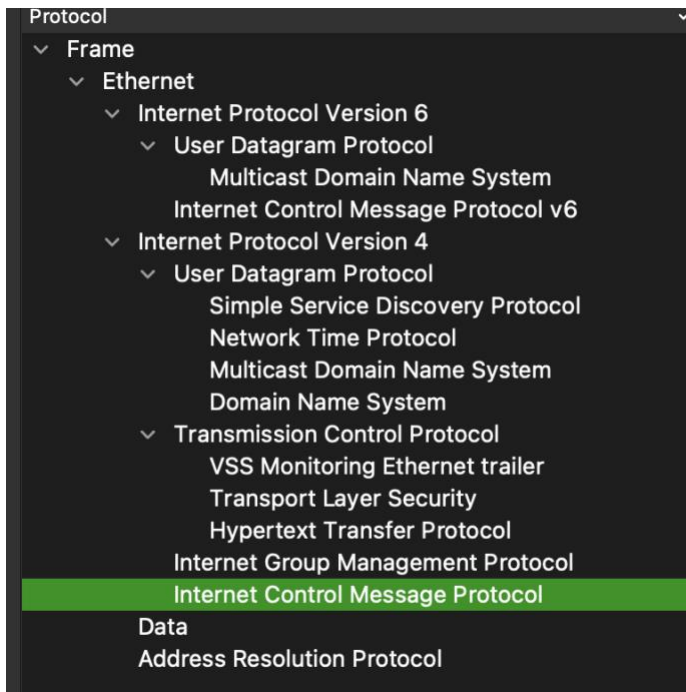
Measurement	Captured	Displayed	Marked
Packets	7766	7766 (100.0%)	—
Time span,s	535.618	535.618	—
Average pps	14.5	14.5	—
Average packet size,B	402	402	—
Bytes	3118522	3118522 (100.0%)	0

3. What protocol is used by ping?

→ uses ICMP protocol

7721	529.750262	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=17/4352, ttl=103 (request in 7715)
7715	529.719633	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=17/4352, ttl=64 (reply in 7721)
7713	528.740248	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=16/4096, ttl=103 (request in 7712)
7712	528.716353	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=16/4096, ttl=64 (reply in 7713)
7703	527.737537	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=15/3840, ttl=103 (request in 7702)
7702	527.713711	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=15/3840, ttl=64 (reply in 7703)
7698	526.733660	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=14/3584, ttl=103 (request in 7697)
7697	526.709267	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=14/3584, ttl=64 (reply in 7698)
7686	525.739345	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=13/3328, ttl=103 (request in 7683)
7683	525.709111	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=13/3328, ttl=64 (reply in 7686)
7675	524.731560	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=12/3072, ttl=103 (request in 7674)
7674	524.707994	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=12/3072, ttl=64 (reply in 7675)
7662	523.737413	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=11/2816, ttl=103 (request in 7661)
7661	523.706963	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=11/2816, ttl=64 (reply in 7662)
7659	522.734332	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=10/2560, ttl=103 (request in 7656)
7656	522.704619	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=10/2560, ttl=64 (reply in 7659)
7649	521.730294	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=9/2304, ttl=103 (request in 7648)
7648	521.700362	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=9/2304, ttl=64 (reply in 7649)
7638	520.723824	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=8/2048, ttl=103 (request in 7635)
7635	520.699575	192.168.1.210	142.250.138.190	ICMP	98	Echo (ping) request	id=8x3d1a, seq=8/2048, ttl=64 (reply in 7638)
7615	519.726164	142.250.138...	192.168.1.210	ICMP	98	Echo (ping) reply	id=8x3d1a, seq=7/1792, ttl=103 (request in 7614)

4. List the protocols used by the captured packets.
 → TLS (TLSv1.3, TLSv1.2), TCP, SSDP, NTP, MDNS, IGMP (IGMPv3), ICMP (ICMPv6, ICMP), HTTP, DNS, ARP, 0x7373



5. Pick one of these protocols which was unfamiliar to you, learn what it does, and give a one-sentence summary in your own words.

igmp							
No.	Time	Source	Destination	Protocol	~ Length	Info	
871	89.337767	192.168.1.254	224.0.0.1	IGMPv3	60	Membership Query, general	
2532	214.371809	192.168.1.254	224.0.0.1	IGMPv3	60	Membership Query, general	
5153	339.398577	192.168.1.254	224.0.0.1	IGMPv3	60	Membership Query, general	
7020	464.433686	192.168.1.254	224.0.0.1	IGMPv3	60	Membership Query, general	

→ IGMP: Internet Group Message Protocol --- This protocol is used to allow a host to advertise its multicast group with neighboring switches and routers, which means it lets to communicate from one source to a selected group of destination.

7. Look at any 3 UDP packets. The header should include the protocol number for UDP, namely 17 (11₁₆). Where does this occur (at what byte number)? Is this the same for each UDP packet? Explain why it occurs here, based the information Wireshark displays and your knowledge of the length and layout of packet headers.

1.

```

2260 199.755300 192.168.1.254 192.168.1.210 DNS 153 Standard query response 0xbce7 HTTPS googlehosted.l.googleusercontent.com SOA ns1.google.com
  Fragment Offset: 0
  Time to Live: 64
  Protocol: UDP (17)
  Header Checksum: 0x01a5 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.254
  Destination Address: 192.168.1.210
  User Datagram Protocol, Src Port: 53, Dst Port: 58782
    Source Port: 53
    Destination Port: 58782
    Length: 119
    Checksum: 0x7e6b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 9]
    [Timestamps]
      [Time since first frame: 0.020640000 seconds]
      [Time since previous frame: 0.020640000 seconds]
    UDP payload (111 bytes)
  Domain Name System (response)
    Transaction ID: 0xbce7
    > Flags: 0x0180 Standard query response, No error
    Questions: 1
    Answer RRs: 0
    Authority RRs: 1
    Additional RRs: 0
    Queries
      > googlehosted.l.googleusercontent.com: type HTTPS, class IN
    Authoritative nameservers
      > l.googleusercontent.com: type SOA, class IN, mname ns1.google.com
        Name: l.googleusercontent.com
        Type: SOA (Start Of a zone of Authority) (6)
        Class: IN (0x0001)
        Time to live: 53 (53 seconds)
        Data length: 45
        Primary name server: ns1.google.com
        Responsible authority's mailbox: dns-admin.google.com
        Serial Number: 369489900
        Refresh Interval: 900 (15 minutes)
        Retry Interval: 900 (15 minutes)
        Expire limit: 1800 (30 minutes)
        Minimum TTL: 60 (1 minute)
    [Request In: 2254]
    [Time: 0.020640000 seconds]
0000  14 7d da 38 5b ab 88 ef 16 75 3c 20 08 00 45 28  .}-8[...u<..E(
0010  00 8b f3 74 00 00 40 11 01 a5 c0 a8 01 fe c0 a8  ...t...@...
0020  01 d2 00 35 e5 9e 00 77 7e 6b bc e7 81 80 00 01  ...5...w~k.....
0030  00 00 00 01 00 00 0c 67 6f 6f 67 6c 65 68 6f 73  ....g ooglehos
0040  74 65 64 01 6c 11 67 6f 6f 67 6c 65 75 73 65 72  ted.l.go ogleuser
0050  63 6f 6e 74 65 6e 74 03 63 6f 6d 00 00 41 00 01  content.com..A..
0060  c0 19 00 06 00 01 00 00 00 35 00 2d 03 6e 73 31  ....5.-ns1
0070  06 67 6f 6f 67 6c 65 c0 2d 09 64 6e 73 2d 61 64  .google-.-dns-ad
0080  6d 69 6e c0 46 16 05 f7 ec 00 00 03 84 00 00 03  min.F...
0090  84 00 00 07 08 00 00 00 3c  ....<

```

2.

```

2032 189.598501 192.168.1.254 192.168.1.210 DNS 144 Standard query response 0xec7b No such name PTR lb._dns-sd._udp.attlocal.net SOA localhost
Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x174f [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.254
Destination Address: 192.168.1.210
User Datagram Protocol, Src Port: 53, Dst Port: 59916
Source Port: 53
Destination Port: 59916
Length: 110
Checksum: 0x4d22 [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[Timestamps]
[Time since first frame: 0.026526000 seconds]
[Time since previous frame: 0.026526000 seconds]
UDP payload (102 bytes)
Domain Name System (response)
Transaction ID: 0xec7b
Flags: 0x8583 Standard query response, No such name
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0
Queries
> lb._dns-sd._udp.attlocal.net: type PTR, class IN
Authoritative nameservers
attlocal.net: type SOA, class IN, mname localhost
Name: attlocal.net
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 3600 (1 hour)
Data length: 44
Primary name server: localhost
Responsible authority's mailbox: postmaster.localhost
Serial Number: 2004052401
Refresh Interval: 3600 (1 hour)
Retry Interval: 1800 (30 minutes)
Expire limit: 604800 (7 days)
Minimum TTL: 3600 (1 hour)
[Request In: 2031]
[Time: 0.026526000 seconds]
0000 14 7d da 38 5b ab 88 ef 16 75 3c 20 08 00 45 28 .}.8[... u< ..E(
0010 00 82 dd d3 00 00 40 11 17 4f c0 a8 01 fe c0 a8 .....@. .0.....
0020 01 d2 00 35 ea 0c 00 6e 4d 22 ec 7b 85 83 00 01 ...5...n M".{....
0030 00 00 00 01 00 00 02 6c 62 07 5f 64 6e 73 2d 73 .....l b._dns-s
0040 64 04 5f 75 64 70 08 61 74 74 6c 6f 63 61 6c 03 d._udp.a ttlocal.
0050 6e 65 74 00 00 0c 00 01 c0 1c 00 06 00 01 00 00 net.....
0060 0e 10 00 2c 09 6c 6f 63 61 6c 68 6f 73 74 00 0a ...,.loc alhost..
0070 70 6f 73 74 6d 61 73 74 65 72 c0 3a 77 73 69 b1 postmast er:wsil
0080 00 00 0e 10 00 00 07 08 00 09 3a 80 00 00 0e 10 .....:.....

```

Protocol (ip.proto), 1 byte

3. 1797 168.397779 192.168.1.123 239.255.255.250 SSDP 353 NOTIFY * HTTP/1.1

```

    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 4
    Protocol: UDP (17)
    Header Checksum: 0x7788 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.123
    Destination Address: 239.255.255.250
    User Datagram Protocol, Src Port: 60000, Dst Port: 1900
    Source Port: 60000
    Destination Port: 1900
    Length: 319
    Checksum: 0x51d5 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 4]
    [Timestamps]
    [Time since first frame: 0.419167000 seconds]
    [Time since previous frame: 0.000001000 seconds]
    UDP payload (311 bytes)
    Simple Service Discovery Protocol
    NOTIFY * HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): NOTIFY * HTTP/1.1\r\n]
    [NOTIFY * HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: NOTIFY
    Request URI: *
    Request Version: HTTP/1.1
    USN: uuid:5235e621-5936-31ef-9865-7a6ac35fa66c::upnp:rootdevice\r\n
    CACHE-CONTROL: max-age=1800\r\n
    NT: upnp:rootdevice\r\n
    HOST: 239.255.255.250:1900\r\n
    LOCATION: http://192.168.49.1:60000/upnp/dev/5235e621-5936-31ef-9865-7a6ac35fa66c/de
    SERVER: Linux/3.10.54 UPnP/1.0 Cling/2.0\r\n
    NTS: ssdp:alive\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]

0010 01 53 4b f4 40 00 04 11 77 88 c0 a8 01 7b ef ff .SK@...w....{..
0020 ff fa ea 60 07 6c 01 3f 51 d5 4e 4f 54 49 46 59 ...l.? Q:NOTIFY
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 55 53 4e * HTTP/ 1.1..USN
0040 3a 20 75 75 69 64 3a 35 32 33 35 65 36 32 31 2d : uuid:5 235e621-
0050 35 39 33 36 2d 33 31 65 66 2d 39 38 36 35 2d 37 5936-31e f-9865-7
0060 61 36 61 63 33 35 66 61 36 36 63 3a 3a 75 70 6e a6ac35fa 66c::upn
0070 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a 43 41 p:rootde vice:CA
0080 43 48 45 2d 43 4f 4e 54 52 4f 4c 3a 20 6d 61 78 CHE-CONT ROL: max
0090 2d 61 67 65 3d 31 38 30 30 0d 0a 4e 54 3a 20 75 -age=180 0 NT: u
00a0 70 6e 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a pnp:root device..
00b0 48 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 HOST: 23 9.255.25
00c0 35 2e 32 35 30 3a 31 39 30 30 0d 0a 4c 4f 43 41 5.250:19 00 LOCA
00d0 54 49 4f 4e 3a 20 68 74 74 70 3a 2f 2f 31 39 32 TION: ht tp://192
00e0 2e 31 36 38 2e 34 39 2e 31 3a 36 30 30 30 30 2f .168.49. 1:60000/
00f0 75 70 6e 70 2f 64 65 76 2f 35 32 33 35 65 36 32 upnp/dev /5235e62
0100 31 2d 35 39 33 36 2d 33 31 65 66 2d 39 38 36 35 1-5936-3 1ef-9865
0110 2d 37 61 36 61 63 33 35 66 61 36 36 63 2f 64 65 -7a6ac35 fa66c/de
0120 73 63 0d 0a 53 45 52 56 45 52 3a 20 4c 69 6e 75 sc..SERV ER: Linu
0130 78 2f 33 2e 31 30 2e 35 34 20 55 50 6e 50 2f 31 x/3.10.5 4 UPnP/1
0140 2e 30 20 43 6c 69 6e 67 2f 32 2e 30 0d 0a 4e 54 .0 Cling /2.0 NT
0150 53 3a 20 73 73 64 70 3a 61 6c 69 76 65 0d 0a 0d S: ssdp: alive...

Protocol (ip.proto): 1 byte

```

→ All of them are 17 indicating that it is an UDP protocol. In addition, all of them occurred on byte 23 and had the number '11'.
Convert 11x to a decimal is: $1 \times 16^1 + 1 \times 16^0 = 16 + 1 = 17$ (UDP protocol number).
The position when protocol occurs is at byte 23.

‘Ethernet II’ contains 14 bytes which is irrelevant to IPv4 Header, and ‘Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.210’ contains 20 bytes which matches with IPv4 header from Version to Destination Address. Within the IPv4 Header, the protocol is located on the 10th. Thus, 14 bytes, “Internet Protocol Version 4’ which comes before IP header information, plus 10 since the order of IPv4 Header format. $10 + 14 = 24$. Counting starts from 0, therefore $24 - 1 = 23$.

With this information, it make sense why it have 11, 17, and location of 23rd byte.

The screenshot displays the Wireshark network protocol analyzer interface. The top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 1356), including the Ethernet II header and the Application Data payload. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1356	120.175260	192.168.1.210	157.240.24.60	TLSv1.2	209	Application Data
1333	118.357583	192.168.1.210	157.240.24.60	TLSv1.2	209	Application Data
346	36.326351	192.168.1.210	157.240.24.60	TLSv1.2	209	Application Data
288	29.104112	192.168.1.210	157.240.24.60	TLSv1.2	209	Application Data
263	24.971913	192.168.1.210	157.240.24.60	TLSv1.2	209	Application Data
216	21.636705	192.168.1.210	157.240.24.60	TLSv1.2	209	Application Data
2474	206.798992	157.240.24.60	192.168.1.210	TCP	208	[TCP Retransmission] 443 → 52424 [PSH, ACK] Seq=16
2473	206.798990	157.240.24.60	192.168.1.210	TLSv1.3	208	Application Data
2471	206.798985	157.240.24.60	192.168.1.210	TLSv1.3	208	Application Data
2470	206.798978	157.240.24.60	192.168.1.210	TLSv1.3	208	Application Data
1460	128.905790	157.240.24.60	192.168.1.210	TLSv1.2	208	Application Data
1301	121.499523	157.240.24.60	192.168.1.210	TLSv1.2	208	[TCP Spurious Retransmission] , Application Data
1377	121.497577	157.240.24.60	192.168.1.210	TLSv1.2	208	Application Data
836	87.502698	192.168.1.210	157.240.24.60	TLSv1.3	208	Application Data
308	39.575221	157.240.24.60	192.168.1.210	TLSv1.2	208	Application Data
6591	438.630668	192.168.1.210	40.89.244.232	TLSv1.3	206	Application Data
6553	438.497321	192.168.1.210	40.89.244.232	TLSv1.3	206	Application Data
6758	442.506283	192.168.1.210	151.101.129.69	TLSv1.2	203	Application Data
6577	438.589922	192.168.1.210	40.89.244.232	TLSv1.3	203	Application Data
2191	198.280440	192.168.1.210	157.240.24.60	TLSv1.3	201	Application Data
795	84.426401	162.159.133...	192.168.1.210	TLSv1.2	195	Application Data
7246	482.612832	54.184.93.203	192.168.1.210	TLSv1.3	194	Application Data
7505	510.125762	192.168.1.210	157.240.24.60	TLSv1.3	193	Application Data
4514	289.017729	162.159.133...	192.168.1.210	TLSv1.2	193	Application Data
2230	199.448780	192.168.1.210	157.240.24.60	TLSv1.3	193	Application Data
1574	144.016850	192.168.1.210	157.240.24.60	TLSv1.2	193	Application Data
522	53.547445	192.168.1.210	157.240.24.60	TLSv1.2	193	Application Data
5210	345.061527	192.168.1.210	165.227.124.183	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted
4659	298.037846	192.168.1.210	52.40.44.71	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted
1748	165.065913	192.168.1.210	165.227.124.183	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted
3001	263.214409	fe80::baef:1...	ff02::1	ICMPv6	190	Router Advertisement from 88:ef:16:75:3c:20
368	37.727491	fe80::baef:1...	ff02::1	ICMPv6	190	Router Advertisement from 88:ef:16:75:3c:20
7214	482.387858	192.168.1.254	192.168.1.210	DNS	189	Standard query response 0xb0c9 HTTPS api-glb-usw2
6860	443.185929	151.101.129...	192.168.1.210	TCP	189	443 → 52501 [PSH, ACK] Seq=46803 Ack=1969 Win=7276
2266	199.760450	192.168.1.254	192.168.1.210	DNS	188	Standard query response 0x72d7 HTTPS p42-caldav.i
2839	248.232615	192.168.1.254	192.168.1.210	DNS	187	Standard query response 0xb861 A time.apple.com.c
7331	494.123067	192.168.1.210	157.240.24.60	TLSv1.3	186	Application Data
5672	395.492093	162.159.133...	192.168.1.210	TLSv1.2	186	Application Data
2248	199.630334	192.168.1.210	157.240.24.60	TLSv1.3	186	Application Data
1308	115.950994	192.168.1.210	157.240.24.60	TLSv1.2	186	Application Data
145	14.046242	192.168.1.210	157.240.24.60	TLSv1.2	186	Application Data
7268	482.693599	54.184.93.203	192.168.1.210	TLSv1.3	185	Application Data
6784	442.614920	151.101.129...	192.168.1.210	TLSv1.2	185	[TCP Previous segment not captured] , Ignored Unk
6779	442.613553	151.101.129...	192.168.1.210	TLSv1.2	185	Application Data, Application Data
5223	345.872281	192.168.1.254	192.168.1.210	DNS	185	Standard query response 0x0901 HTTPS api.cryptocu
7162	481.568778	3.132.204.55	192.168.1.210	TLSv1.3	184	Application Data
5208	345.057082	165.227.124...	192.168.1.210	TLSv1.2	183	Server Key Exchange, Server Hello Done
1746	165.060950	165.227.124...	192.168.1.210	TLSv1.2	183	Server Key Exchange, Server Hello Done
5111	334.506098	192.168.1.210	64.4.54.254	TLSv1.2	182	Application Data
6762	442.581868	151.101.129...	192.168.1.210	TLSv1.2	180	Application Data, Application Data
6783	442.614917	151.101.129...	192.168.1.210	TCP	179	[TCP Previous segment not captured] 443 → 52501 [P
4692	298.215852	35.186.227.1...	192.168.1.210	TLSv1.3	179	Application Data
7286	482.256969	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
6140	422.204039	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
5426	362.152372	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
4745	302.084738	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
2795	242.035273	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
1977	181.977396	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
1385	121.924778	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
618	61.864246	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
326	33.338729	162.159.133...	192.168.1.210	TLSv1.2	178	Application Data
31	1.087303	192.168.1.210	142.250.191.110	HTTP	178	GET /generate_204 HTTP/1.1
3242	281.223757	192.168.1.254	192.168.1.210	DNS	177	Standard query response 0x9c10 HTTPS www.ecb.europ
2937	258.299953	fe80::18fe:1...	ff02::fb	MNMS	177	Standard query 0x0000 PTR _companion-Link._tcp.loc
2853	249.086589	fe80::18fe:1...	ff02::fb	MNMS	177	Standard query 0x0000 PTR _companion-Link._tcp.loc
2826	246.014435	fe80::18fe:1...	ff02::fb	MNMS	177	Standard query 0x0000 PTR _companion-Link._tcp.loc
2819	245.092788	fe80::18fe:1...	ff02::fb	MNMS	177	Standard query 0x0000 PTR _companion-Link._tcp.loc
6499	438.047800	184.16.244.78	192.168.1.210	TLSv1.2	171	Application Data
2231	109.448992	192.168.1.210	157.240.24.60	TLSv1.3	170	Application Data
7123	481.343188	192.168.1.254	192.168.1.210	DNS	168	Standard query response 0xe12e HTTPS api.smoot.app
4617	297.873536	192.168.1.210	184.16.249.249	TLSv1.2	165	Application Data
4755	302.515112	192.168.1.210	157.240.24.60	TLSv1.3	162	Application Data
1343	118.791013	157.240.24.60	192.168.1.210	TLSv1.2	162	Application Data
6175	423.960539	34.107.247.1...	192.168.1.210	TLSv1.3	161	Application Data

Identification: 0xb942 (47426)
Flags: 0x40, Don't fragment
0... = Reserved bit: Not set

0000 14 7d da 3b 5b ab 88 ef 16 75 3c 20 00 00 45 6c .).8[...uc-El
0010 00 c2 b9 42 00 00 57 06 f0 e0 9d f0 18 3c c0 a8 ...00-W-.....
0020 01 d2 01 bb cc 78 8f 73 30 90 ad cd 46 bf 80 18 ...x-s 0...F...
0030 01 8a 3a 8b 00 00 01 01 08 0a df 45 e9 33 23 b2 ...:....E-3#...
0040 4f 20 17 03 03 00 89 6b 77 7f 01 29 d0 81 f4 29 0 ...kww-)...
0050 8d dd 00 84 09 11 d4 fa 68 99 b4 f2 5e 80 95 46 ...h-...F...
0060 dd cf 4e 22 20 38 4c 30 fb e9 29 27 e9 db 66 58 ...N)8L0-)-fX...
0070 cf bc 18 8f b6 7a 61 ff 72 75 27 25 d8 94 95 8e ...za:ru'k...
0080 20 b2 a7 4d 93 14 87 e9 6a 2b 9b 89 c3 e1 e0 01 ...M...j+...
0090 12 79 ff 0c 7e 22 8c 86 6f ac f7 5c 65 7f 22 9d ...y-...o-^e-...
00a0 52 e9 52 8b 5b 7d 92 aa e1 ea e9 03 19 1b 28 bb R.R-{}:....(-
00b0 ed c8 72 e8 5d 3a 95 49 96 fb 8c cb 9c e6 7a ...r-}:I-...~z...
00c0 51 b0 d3 bf af bf 3a 17 5e 4a 38 f1 1f 0d ef Q.....~J8...

Reserved bit (p.flags.rb), 1 byte
Packets: 7766 - Displayed: 7766 (100.0%) - Dropped: 0 (0.0%) - Profile: Default

Picture of a wireshark screen for Question 1.